City of Kirkland RFP

Web Content Filtering and/or IDS/IPS Solutions

Vendor Questions and Answers

Released September 19, 2013

1. How many seats are you guys looking to deploy to?
   Answer:
   - 2 Separate wireless segments
     - 200 for Public Wireless
     - 100 for Corporate Wireless
   - 1 Wired Segment
     - 700 Users
   - The preference would be that this can be handled by one appliance or software solution that would handle 700 concurrent connections though

2. Can you provide a network diagram and an idea of areas on that diagram that IDS/IPS protection is desirable?
   Answer: Yes, upon submission of the NDA we can provide a network diagram. Areas of desirable protection would include Kirkland City Hall, the Bellevue Data Center and new public safety building equipment (coming soon).

3. What are the bandwidth requirements for an IDS/IPS solution in the areas that it would be placed?
   Answer: The boarder is the most important with an option for the LAN
   - 100MB Border
   - 10G on the internal LAN

4. Can you provide a sample configuration, based on your network, that would allow us to specify and provide quoting information that is consistent for a true comparison?
   Answer: See question #2

5. What technical requirements/features are needed at City of Kirkland for an IDS/IPS solution? Are there any must haves, desirables, do not wants?
   Answer: We would like to a menu of what you have to offer, including, but not limited to such things as being warned of ping sweeps, DoS attacks and the ability to monitor an analyze IP traffic.

6. Do you want or need malware protection on the network and/or integrated with your endpoints?
   Answer: Yes. We would like the solutions to include monitoring removable media such as USB drives or external HDs.

7. Does the solution need to have the ability to adapt to network changes without administrator intervention?
   Answer: This would be a nice to have – for example if certain thresholds are passed.

8. Is the ability to dynamically inspect uncategorized web content with real-time content examination and analysis of websites to determine the risk level of each and every webpage as it attempts to enter your network a must have or nice to have? If it is not a must, is URL based web filtering going to suffice?
   Answer: This is a must have.

9. Do you need the ability to set granular policies for individuals and groups to restrict web liabilities, bandwidth consumption, threats, prevent data leakage or exposure of sensitive or confidential data-in-motion across web channels or email?
   Answer: Yes

10. Do you need the devices to be set up in HA or is the ability to fail-open to prevent traffic loss upon failure sufficient?
    Answer: HA is preferred.

11. If available, are you interested in bundling a firewall into the solution as well?
    Answer: Probably not. We just purchased new HA CISCO 5525's and are not likely to replace them as part of this project. If you have a compelling case for this, please present it.

12. How large is the environment to be protected?
    - How many Datacenters? 2 physical configured as one logical
    - How Many large sites (Over 1,000 systems)? None
    - How Many medium sites (Between 100 – 1000 systems)? See answer for Windows Server below.
    - How Many small sites (under 100 systems)? 2
    - How Many connected hosts of each type total are there?
        - ○ Windows Workstation (Incl. Windows XP, Windows 7, Windows 8) 250
        - ○ Windows Server (incl: 2003, 2008, 2012) 75
        - ○ Linux (Identify distribution and kernel versions) 7
        - ○ HPUX 0
        - ○ Solaris 0
        - ○ ESX 4
        - ○ AIX 0

13. How Many internet egress points are there?
    Answer: 2 (One Corporate and one Public)

14. What (if any regulatory or compliance drivers must be met by the proposed solution(s)?
    Answer: PCI, HIPPS and CJIS

15. IDS/IPS Solution:
    - Is the request for a host-based IPS/IDS Solution, or for a network-based solution?
      Answer: Network is a must but we would be willing to look at host based as an integrated part of the overall solution
    - If this is a network-based solution, is the scope to include access layer and perimeter coverage, or perimeter coverage only?
      Answer: Perimeter is a must but we would like to weigh all the options for access layer as well.
    - If this is a host-based solution, what types of systems are in scope for intrusion prevention, based on the following categories:
        - Domain Controllers (Servers) – in scope
        - MSSQL Database Server (Servers) – in scope
        - Oracle Database Servers (Servers)
        - MySQL Database Servers (Servers) – in scope
        - Application Servers (Specify application, Servers) Mostly .NET, IIS and Java bases systems– in scope
        - EMail Servers (Specify Type, Servers) Exchange 2010 – in scope
        - Kiosk Systems
        - End-User Desktops – in scope

16. Web Filtering Solution:
    - What Capabilities are being pursued, based on the following categories:
        - URL Filtering
        - Malware Filtering
        - Botnet Detection
        - Content Filtering
        - Data Loss Monitoring/Prevention

          Answer: We are looking for respondents to present us with the capabilities.

17. What kind of users (do they use internet full time)?
    Answers: Not sure what full time means. Our users use the internet throughout the day as part of daily operations.

18. How will you deploy (Explicit/Client Proxy Settings, WCCP)?
    Answers: Preferably transparent authentication via WCCP. Explicit and Client proxy tend to provide poor performance.

19. How many locations (internet egress)?
    Answers: 1 location with 2 egress points

20. How much redundancy? (N+1?)
    Answers: It depends on the solution, but an HA pair is preferred.

21. Do you want authentication?
    Answers: Yes, Transparent is far preferred using the existing MS Active Directory (LDAP is fine as well) though.

22. Do you want complex filtering for URL's per department or group?
    Answers: Yes, we need to be able to define policies based on departments or groups as well as network Segment.

23. Do you want SSL scanning?
    Answers: Yes

24. How many requests/second will you have at sustained and peak times?
    Answers: Currently, we have as many 5,000 requests per second.

25. Do you require Redundant Power or RAID?
    Answers: Power yes and RAID if it is available in the proposed solution

26. What level of training are you looking for on the product?
    Answers: Will depend on the purposed solution. But, training must include at a minimum, Administrator training.